UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/043,546	01/10/2002	Takeshi Yoshimura	15689.95	7337

22913 7590 01/11/2006

WORKMAN NYDEGGER
(F/K/A WORKMAN NYDEGGER & SEELEY)
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/043,546	YOSHIMURA ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,7,11 and 14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *2,7,11 and 14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on October 12, 2005. **Claims 1,3-6, 8-10,12-13 and 15-17 have been canceled and claims 2,7,11 and 14 are** amended. **Claims 2,7,11 and 14** are pending.

Response to Argument

2. Applicant's remark/arguments filed on October 12, 2005, have been fully considered but they are not persuasive.

Applicant's first argument is regarding the amended claims

Applicant's argument is based on the amended claims and argued that the newly added limitation which is submitted is not suggested/discussed by **the references** on the record, either by the primary reference Barnes or by the combinations of the primary and secondary reference Barnes and Ishibashi. Applicant wrote the following in support of his argument,

(B)

"Barnes discloses apparatus extracting information ~~dem~~ from the header of a received packet, deciding if the information extracted is stored in a key list, and encrypting/decrypting the packet according to the decision. In the encryption process of Barnes, a device can be made sensitive to control sequences which place the device in an out of an encryption mode. The control sequences can be entered between the start (STX) and end (ETX) of the message. Hence, the device can encrypt selected portions of the message and leave other portions to be transmitted in plain text.

However, each object of Barnes is different from that of present invention. **The object of Barnes is to provide transparent and secure communications between computer systems or LANS connected to an open network** .On the

other hand, the object of the present invention is to prevent a cryptographic key or authentication key from being broken. For example, when a short packet section is intruded, it will be easily broken. In the present invention, a bit stream with a small number of bits or a bit stream that can be cryptanalyzed easily is not encrypted as recited in Claims 2 and 11.The same is equally true of the invention recited in Claims 7 and 14, in which the type of the bit stream is determined by the number of bits or a degree of effect of tampering.

As discussed above, **the purpose of the present invention is never disclosed in Barnes. Also, no one or ordinary skill in the art would not think of the selective encryption and authentication as recited in Claims** 2, 7, 11 and 14, even in light of Barnes and Ishibashi."

Examiner disagrees with the above argument,

The argument raised by the applicant is based on the comparison of the purpose and advantage that application provides over the reference on the record.

In response to the above argument by the applicant, the Examiner point out the following.

The purpose/advantage of the invention that could be provided by the invention over the prior art cannot be read into the claims. In fact, though the advantage of the invention is implicitly/inherently assumed to be described in the specification by the applicant, the specification is not the measure of the invention. Therefore, limitations contained therein/assumed to be contained therein cannot be read into the claims for the purpose of avoiding the prior art. (See In re Sporck, 55 CCPA 743, 386 F 2d 924, 155 USPQ 687 (1968))

As to the argument raised by the applicant to "**no one or ordinary skill in the art would not think of the selective encryption and authentication as recited in Claims** 2, 7, 11 and 14, even in light of Barnes

and Ishibashi," the examiner would point out that it is not necessary that the reference actually suggest, expressly or in so many words, the changes or improvements that applicant has made. The text for combining references is what the references as a whole would have suggested to one of ordinary skill in the art. See In re Sheckle, 168 USPQ 716 (CCPA 1971) In re McLaghin 170 USPQ 209 (CCPA 1971). In re Young 159 USPQ 725 (CCPA 1968).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims** are rejected under 35 U.S.C. 103(a) as being unpatentable over by **Barnes et al.** (hereinafter referred as **Barnes**)(U.S. Patent 4,159,468), in view of **Ishibashi** (hereinafter referred to as **Ishibashi**) (U.S. Patent 6,021,199).

5. **As per claims 2,7,11 and 14 Barnes** discloses an encryption apparatus for encrypting and transmitting a bit stream of media information [column 4, lines 19-21] (**Plain text**) which is sent from a transmitting terminal, said encryption apparatus comprising:

Means for deciding the number of bits or difficulty in cryptanalysis of the bit stream; [Column 10, lines 2-4] **("When the start of the text (STX) and end of**

the text (ETX) is present in a message, it indicate/define the type of message which should be encrypted meet the recitation of deciding a "the number of bits") and

Means for encrypting the bit stream in which is decided as longer or more difficult to cryptanalyze than a predetermined criterion by means of deciding. [Column 10, lines 2-4; column 10, lines 14-16] (**The device will begin the encryption process on the detection of STX, and end the process on the detection of ETX meets the recitation of encrypting the bit stream in accordance with "the number of bits" decided/detected by said deciding means. Hence the device can selectively encrypt selected portions of the message and leave other portions to be transmitted in plain text as explained on column 10, lines 14-16 and this inherently includes the number of bits that is decided to be encrypted**)

Barnes does not explicitly disclose means of deciding by the difficulty to cryptanalsis of the bit stream and means for encrypting the bit stream in which is decided as more difficult to cryptanalyze than a predetermined criterion.

The office has interpreted this particular limitation in the eye's of the applicant's specification. The following has been recited in the applicant specification in relation to this limitation.

" Among the three types of pictures, the I-pictures 406 are an intra-frame codedpicture, from which the original bit stream can be easily restored if this type of the bit stream is broken. On the other hand, the P-pictures 402 and B-pictures 404 are a prediction coding picture consisting of the difference data between multiple motion pictures. Accordingly, it is difficult to restore the original media information even if only the bit stream of these types are cryptanalyzed. Thus, the encryption/authentication selector 102 in the encryption/authentication assignment apparatus 100 as shown in FIG. 3 decides the picture type of the motion picture data to be transmitted. **Then, the encrypting section 104 encrypts it when it is the I-picture 406. On the other hand, as for the P-pictures 402 and B-pictures 404, they are transmitted without being transformed through the encryption**"

However, in the same field of endeavor, **Ishibashi** discloses, the same features as explained on the abstract as recited as "Of I, P and B pictures contained in an MPEG 2 data stream, only the I picture is subjected to encryption such as scramble processing." [See Abstract, first 3 lines.]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of selectively encrypting as per teachings of **Ishibashi** in to the method of encryption/authentication as taught by **Barnes**, in order to provide efficiency and copy protection/security simultaneously. [See **Ishibashi** column 2, lines 7-21]

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
12/28/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100